Distributed Denial of Service (DDoS)

239.5k views

DDoS

DDoS meaning: What is DDoS?

Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

Unlike other kinds of cyberattacks, DDoS assaults don't attempt to breach your security perimeter. Rather, a DDoS attack aims to make your website and servers unavailable to legitimate users. DDoS can also be used as a smokescreen for other malicious activities and to take down security appliances, breaching the target's security perimeter.

A successful distributed denial of service attack is a highly noticeable event impacting an entire online user base. This makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists and anyone else looking to make a point or champion a cause.

DDoS attacks can come in short bursts or repeat assaults, but either way the impact on a website or business can last for days, weeks and even months, as the organization tries to recover. This can make DDoS extremely destructive to any online organization. Amongst other things, DDoS attacks can lead to loss of revenues, erode consumer trust, force businesses to spend fortunes in compensations and cause long-term reputation damage.

DoS vs. DDoS

The differences between regular and distributed denial of service assaults are substantive. In a DoS attack, a perpetrator uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests—usually in an attempt to exhaust server resources (e.g., RAM and CPU).

On the other hand, distributed denial of service (DDoS) attacks are launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved. Unlike single-source DoS assaults, DDoS attacks tend to target the network infrastructure in an attempt to saturate it with huge volumes of traffic.

DDoS attacks also differ in the manner of their execution. Broadly speaking, denial of service attacks are launched using homebrewed scripts or DoS tools (e.g., Low Orbit Ion Canon), while DDoS attacks are launched from botnets — large clusters of connected devices (e.g., cellphones, PCs or routers) infected with malware that allows remote control by an attacker.

DDoS botnets: waging large-scale attacks

A botnet is a collection of hijacked connected devices used for cyber attacks that are controlled remotely from a Command & Control Center (C&C). These typically include personal computers, mobile phones, unsecured IoT devices, and even resources from public cloud services. Attackers use malware and other techniques to compromise a device, turning it into a "zombie" in the attacker's botnet.

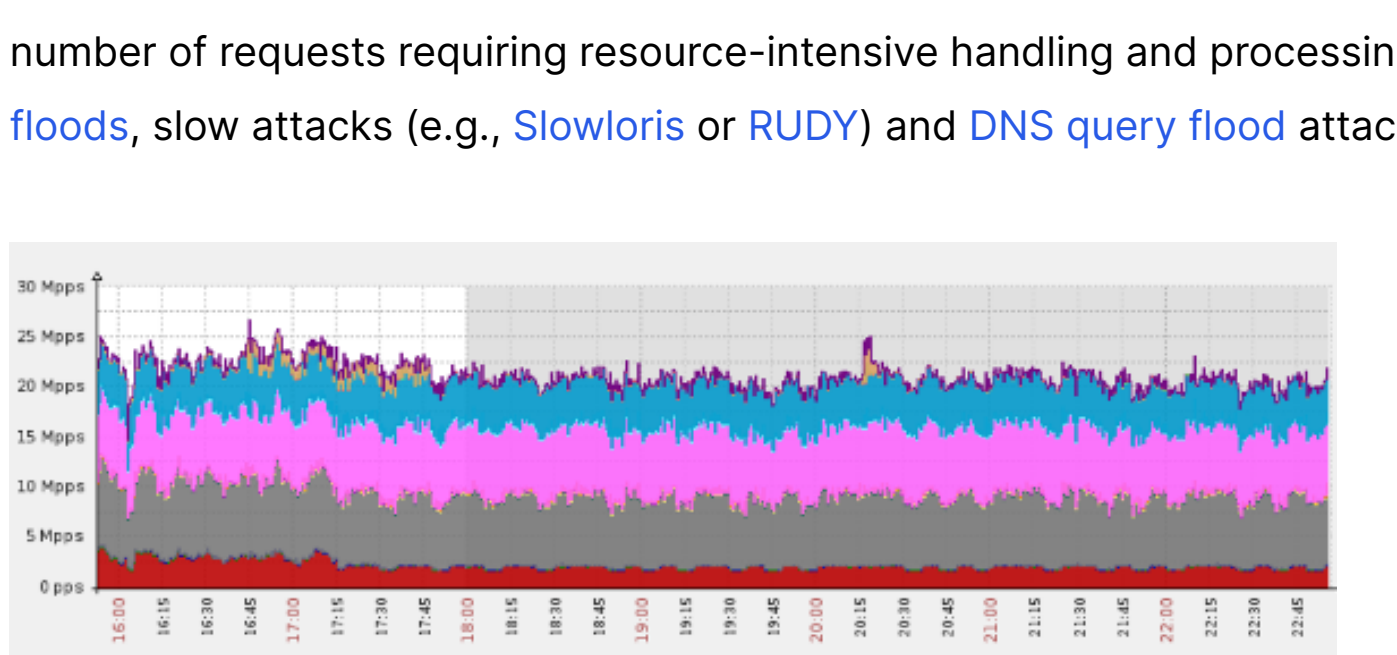
Botnets enable attackers to carry out DDoS attacks by harnessing the power of many machines and obscuring the source of the traffic. Since traffic is distributed, it is difficult for security tools and teams to detect that a DDoS attack is occurring until it is too late.

To learn more about large-scale DDoS infrastructure, see our article on DDoS botnets.

Types of DDoS attacks

DoS attacks can be divided into two general categories—application layer attacks and network layer attacks. Each of these types of DDoS attacks define certain parameters and behaviors used during the attack, as well as the target of the attack.

1. Application layer attacks (a.k.a., layer 7 attacks) can be either DoS or DDoS threats that seek to overload a server by sending a large number of requests requiring resource-intensive handling and processing. Among other attack vectors, this category includes HTTP floods, slow attacks (e.g., Slowloris or RUDY) and DNS query flood attacks.



Gaming website hit with a massive DNS flood, peaking at over 25 million packets per second

The size of application layer attacks is typically measured in requests per second (RPS), with no more than 50 to 100 RPS being required to cripple most mid-sized websites.

2. Network layer attacks (a.k.a., layer 3–4 attacks) are almost always DDoS assaults set up to clog the "pipelines" connecting your network. Attack vectors in this category include UDP flood, SYN flood, NTP amplification and DNS amplification attacks, and more.

Any of these can be used to prevent access to your servers, while also causing severe operational damages, such as account suspension and massive overage charges.

DDoS attacks are almost always high-traffic events, commonly measured in gigabits per second (Gbps) or packets per second (PPS). The largest network layer assaults can exceed hundreds Gbps; however, 20 to 40 Gbps are enough to completely shut down most network infrastructures.

Reasons for DDoSing: Attacker motivations

"DDoSsing" describes the act of carrying out a DDoS attack. Denial of service attacks are launched by individuals, businesses and even nation-states, each with their own motivation.

Hacktivism

Hacktivists use DoS attacks as a means to express their criticism of everything, from governments and politicians, including "big business", and current events. If hacktivists disagree with you, your site is going to go down (a.k.a., "tango down").

Less technically-savvy than other types of attackers, hacktivists tend to use premade tools to wage assaults against their targets. Anonymous is perhaps one of the best-known hacktivist groups. They're responsible for the cyber attack in February 2015 against ISIS, following the latter's terrorist attack against the Paris offices of Charlie Hebdo, as well as the attack against the Brazilian government and World Cup sponsors in June 2014.

Typical assault method of hacktivists: DoS and DDoS.

Cyber vandalism

Cyber vandals are often referred to as "script kiddies"—for their reliance on premade scripts and tools to cause grief to their fellow Internet citizens. These vandals are often bored teenagers looking for an adrenaline rush, or seeking to vent their anger or frustration against an institution (e.g., school) or person they feel has wronged them. Some are , of course, just looking for attention and the respect of their peers.

Alongside premade tools and scripts, cyber vandals will also result to using DDoS-for-hire services (a.k.a., booters or stressers), which can be purchased online for as little as $19 a pop.

Extortion

An increasingly popular motivation for DDoS attacks is extortion, meaning a cybercriminal demands money in exchange for stopping (or not carrying out) a crippling DDoS attack. Several prominent online software companies—including MeetUp, Bitly, Vimeo, and Basecamp—have been on the receiving end of these DDoS notes, some going offline after refusing to succumb to the extortionists' threats.

Similar to cyber-vandalism, this type of attack is enabled by the existence of stresser and booter services.

Typical assault method of extortionists: DDoS.

Business competition

DDoS attacks are increasingly being used as a competitive business tool. Some of these assaults are designed to keep a competitor from participating in a significant event (e.g., Cyber Monday), while others are launched with a goal of completely shutting down online businesses for months.

One way or another, the idea is to cause disruption that will encourage your customers to flock to the competitor while also causing financial and reputational damage. An average cost of a DDoS attack to an organization can run at $40,000 per hour.

Business-feud attacks are often well-funded and executed by professional "hired guns," who conduct early reconnaissance and use proprietary tools and resources to sustain extremely aggressive and persistent DDoS attacks.

Typical assault method used by business competitors: DDoS.

Cyber warfare

State-sponsored DDoS attacks are being used to silence government critics and internal opposition, as well as a means to disrupt critical financial, health, and infrastructure services in enemy countries.

These attacks are backed by nation-states, meaning they are well-funded and orchestrated campaigns that are executed by tech-savvy professionals.

Typical assault method employed as cyber warfare: DDoS.

Personal rivalry

DoS attacks can be used to settle personal scores or to disrupt online competitions. Such assaults often occur in the context of multiplayer online games, where players launch DDoS barrages against one another, and even against gaming servers, to gain an edge or to avoid imminent defeat by "flipping the table."

Attacks against players are often DoS assaults, executed with widely available malicious software. Conversely, attacks against gaming servers are likely to be DDoS assaults, launched by stressers and booters.

Typical assault method of personal rivals: DoS, DDoS.

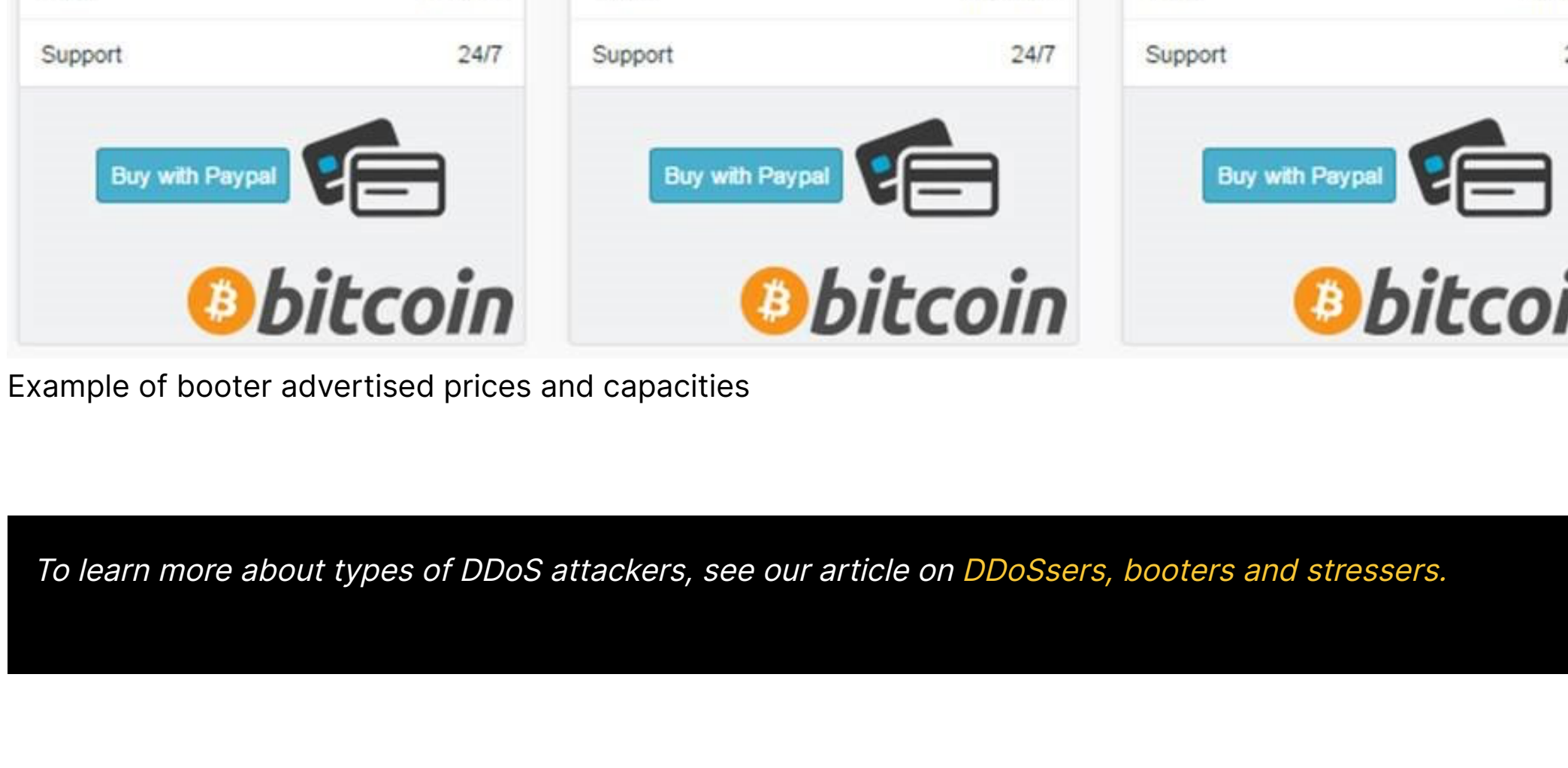
Read our article to learn more about DDoSing in online gaming.

DDoS for hire: DDoSsers, booters and stressers

DDoS for hire providers offer to perform DDoS attacks on the behalf of others for payment. These threat actors are known by multiple names, including DDoSser, booters, and stressers. The wide availability of DDoS for hire makes it possible for almost anyone to wage large-scale attacks.

One reason actors may go by a particular name is to appear as a legal service. For example, stressers typically claim to offer services for stress testing server resilience. However, these actors of do not verify the owner of the server they are "testing" to ensure tests are legitimate.

In contrast, actors who refer to themselves as booters and DDoSsers typically don't try to hide the illegal nature of their services.



$23.99 1 month		$34.99 1 month		$44.99 10 years	
1 Month Gold		1 Month Diamond		Lifetime Bronze	
Time per boot	2400 sec	Time per boot	3600 sec	Time per boot	600 sec
Concurrents	1	Concurrents	2	Concurrents	2
Total network	220Gbps	Total network	220Gbps	Total network	220Gbps
Tools	Included	Tools	Included	Tools	Included
Support	24/7	Support	24/7	Support	24/7

Example of booter advertised prices and capacities

To learn more about types of DDoS attackers, see our article on DDoSsers, booters and stressers.

How to stop DDoS attacks: DIY

You can't prevent DoS assaults. Cybercriminals are going to attack. Some are going to hit their targets, regardless of the defenses in place. However, there are a few preventive measures you can take on your own:

- Monitoring your traffic to look for abnormalities, including unexplained traffic spikes and visits from suspect IP address and geolocations. All of these could be signs of attackers performing "dry runs" to test your defenses before committing to a full-fledged attack. Recognizing these for what they are can help you prepare for the onslaught to follow.
- Keep an eye on social media (particularly Twitter) and public waste bins (e.g., Pastebin.com) for threats, conversations and boasts that may hint on an incoming attack.
- Consider using third-party DDoS testing (i.e., pen testing) to simulate an attack against your IT infrastructure so you can be prepared when the moment of truth arrives. When you undertake this, test against a wide variety of attacks, not just those with which you are familiar with.
- Create a response plan and a rapid response team, meaning a designated group of people whose job is to minimize the impact of an assault. When you plan, put in place procedures for your customer support and communication teams, not just for your IT professionals.

To truly protect against modern DDoS attacks, you should use a DDoS mitigation solution. Solutions can be deployed on-premises, but are more commonly provided as a service by third-party providers. We explain more about DDoS mitigation services in the following section.

To learn more about DIY, on-premise, and cloud service approaches to DDoS protection, see our article on how to stop DDoS attacks.

DDoS mitigation: How does anti-DDoS protection work?

This first step in selecting a DDoS mitigation solution is to assess your risk. Important basic questions include:

- Which infrastructure assets need protection?
- What are the soft spots, or single points of failure?
- What is required to take them down?
- How and when will you know you're targeted? Will it be too late?
- What are the impacts (financial and otherwise) of an extended outage?

Armed with this information, it's then time to prioritize your concerns, examining various DDoS mitigation options within the framework of your security budget.

If you're running a commercial website or online applications (e.g., SaaS applications, online banking, e-commerce), you're probably going to want 24×7, always-on protection. A large law firm, on the other hand, may be more interested in protecting its infrastructure—including email servers, FTP servers, and back office platforms—than its website. This type of business may opt for an "on demand" solution.

The second step is to choose the method of deployment. The most common and effective way to deploy on-demand DDoS protection for your core infrastructure services across an entire subnet is via border gateway protocol (BGP) routing. However, this will only work on demand, requiring you to manually activate the security solution in case of an attack.

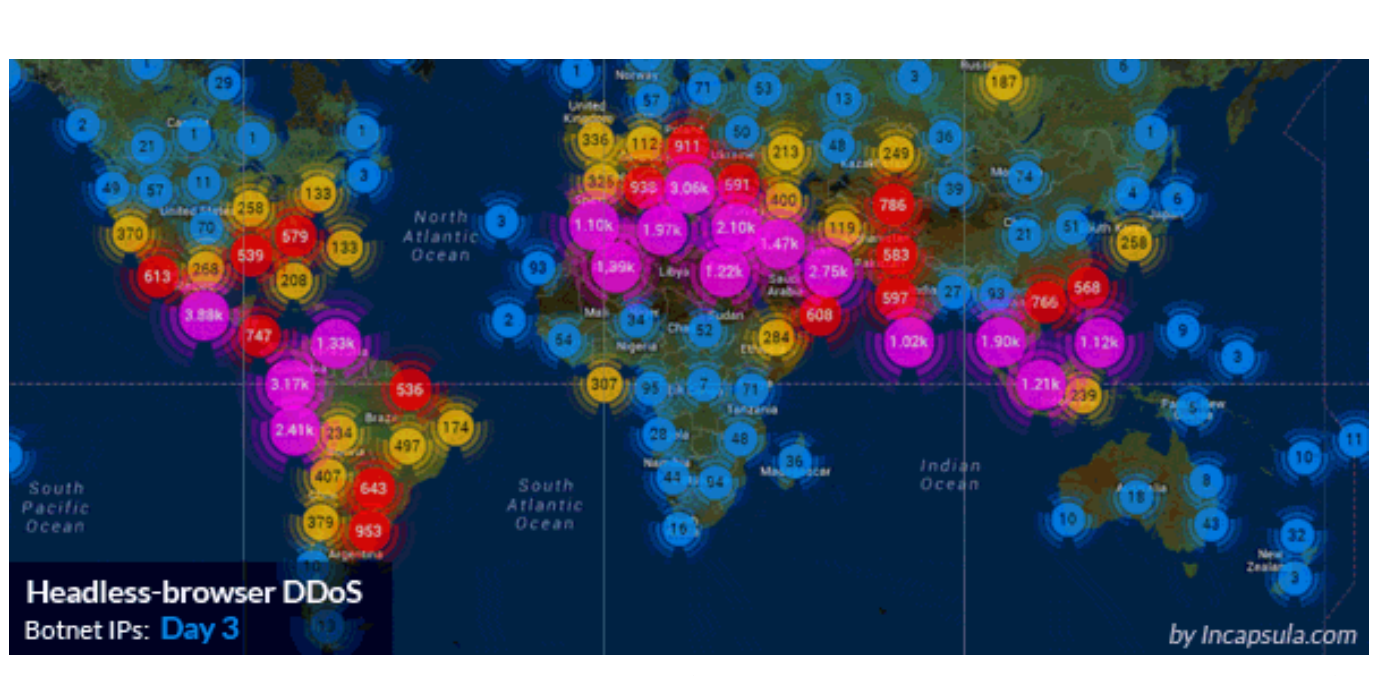
Consequently, if you're in need of always-on DDoS protection for your web application, you should use DNS redirection to reroute all website traffic (HTTP/HTTPS) through your DDoS protection provider's network (usually integrated with a content delivery network,). The advantage of this solution is that most CDNs offer on-call scalability to absorb volumetric attacks, at the same time minimizing latency and accelerating content delivery.

Mitigating Network Layer Attacks

Dealing with network layer attacks required requires additional scalability—beyond what your own network can offer.

Consequently, in the event of an assault, a BGP announcement is made to ensure that all incoming traffic is routed through a set of scrubbing centers. Each of these has the capacity to process hundreds of Gbps worth of traffic. Powerful servers located in the scrubbing centers will then filter out malicious packets, only forwarding the clean traffic to the origin server through a GRE tunnel.

This method of mitigation provides protection against direct-to-IP attacks and is usually compatible with all types of infrastructures and communication protocols (e.g., UDP, SMTP, FTP, VoIP).

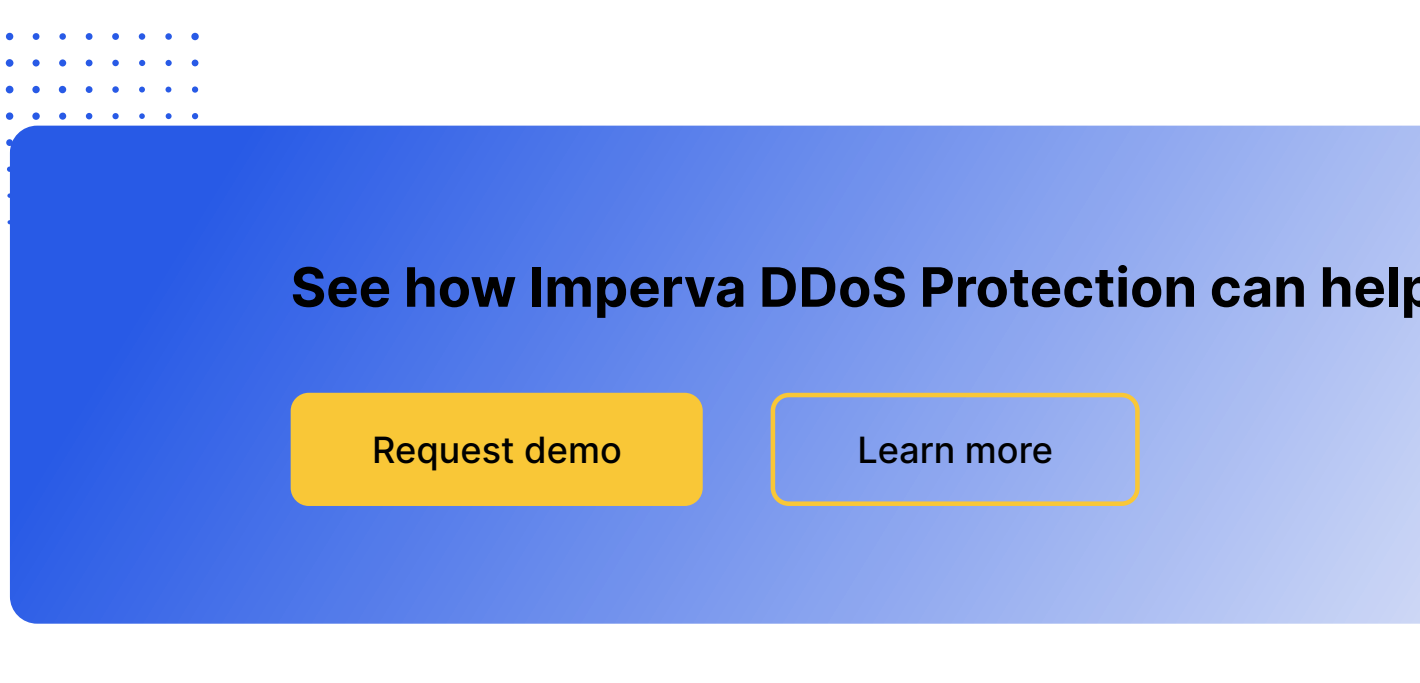


Protecting against an NTP amplification attack: 180Gbps and 50 million packets per second

Mitigating Application Layer Attacks

Mitigation of application layer attacks relies on traffic profiling solutions that can scale on demand, while also being able to distinguish between malicious bots and legitimate website visitors.

For traffic profiling, best practices call for signature-based and behavior-based heuristics, combined with IP reputation scoring and a progressive use of security challenges (e.g., JS and cookie challenges).



Mitigating an eight day-long HTTP flood: 690 million DDoS requests from 180,000 botnets IPs

Together, these accurately filter out malicious bot traffic, protecting against application layer attacks without any impact to your legitimate visitors.

To learn more about how third-party DDoS services work, see our articles on: DDoS mitigation and Anti-DDoS protection

See how Imperva DDoS Protection can help you with DDoS attacks.

Request demo Learn more

DDoS protection by Imperva

Imperva offers a DDoS protection solution that mitigates large-scale DDoS attacks quickly, without disrupting service to legitimate users. Imperva provides protection for websites and web applications, networks and subnets, domain name servers (DNS), and individual IP addresses.

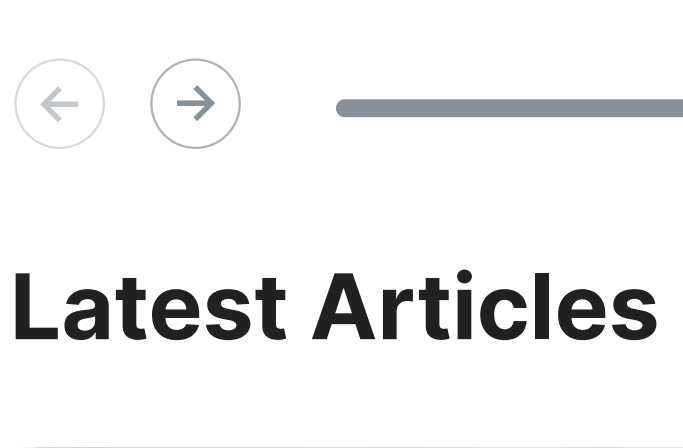
Imperva detects and mitigates any type of DDoS attack, including TCP SYN+ACK, TCP Fragment, UDP, Slowloris, Spoofing, ICMP, IGMP, HTTP Flood, Brute Force, Connection Flood, DNS Flood, NXDomain, Ping of Death, Smurf, Reflected ICMP & UDP.

Imperva DDoS protection provides:

- **Support for Anycast and Unicast**, enabling you to automatically detect and respond to attacks and vulnerabilities.
- **An SLA-backed guarantee** that attacks are blocked in three seconds or less, preventing outage and reducing recovery time.
- **A high-capacity network** capable of analyzing over 65 billion packets per second.
- **Live dashboards** allowing you to see the current status, identify DDoS attacks and understand the parameters of an attack.

Learn more about Imperva's DDoS protection solution.

Latest Blogs



Application Security

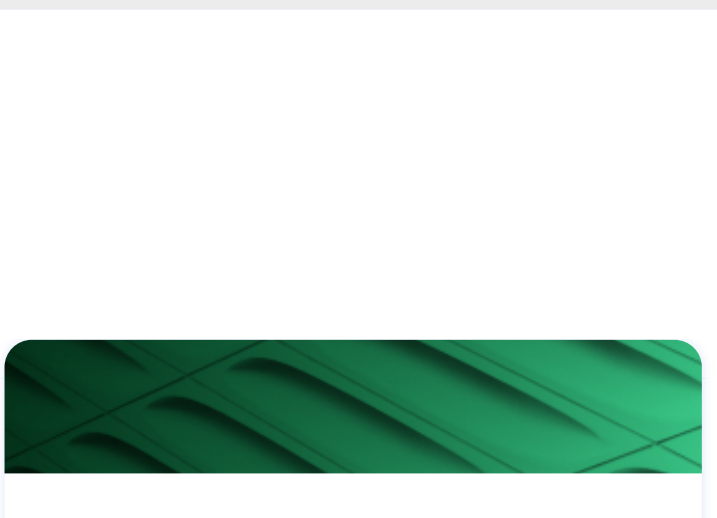
Five Key Takeaways from the 2024 Imperva Bad Bot Report

Erez Hasson
Apr 16, 2024 | 4 min read

Application Security

Understanding the OWASP API Security Top 10: Why BOLA is the Number One[...]

Grainne McKeever
Mar 13, 2024 | 2 min read



Application Security

Latest Research Reveals Rise in API Attacks in 2023, Putting Businesses at[...]

Grainne McKeever
Feb 26, 2024 | 3 min read

Application Security

Are You Ready for

Erez Hasson
Jan 18, 2024 |

Latest Articles

Network Security

DDoS Attacks

440.6k Views

Network Security

Booters, Stressers and DDoSers

314k Views

Network Security

TCP SYN Flood

261k Views

Network Security

Ping flood (ICMP f

213.7k Views

imperva
a Thales company
+1 866 926 4678

Partners
Imperva Partner Ecosystem
Channel Partners
Technology Alliances
Find a Partner
Partner Portal Login

Support
Emergency DDoS Protection
Support Portal
Imperva Community
Documentation Portal
API Integration
Trust Center

Network
Network Map
System Status

Resources
Imperva Blog
Resource Library
Case Studies
Learning Center

About Us
Why Imperva
Who We Are
Events
Careers
Press & Awards
Contact Information

Cookies Settings
Trust Center
Modern Slavery Statement
Privacy
Legal
English

Copyright © 2024 Imperva. All rights reserved